Cyber Liability: Internet Killed the Radio Star

By Erin Gloeckner

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity, Insurance and Risk Financing

Remember the first music video that premiered on MTV? The Buggles' "Video Killed the Radio Star" questioned the impact of new technology on the music industry. Technology and music videos have come a long way since then, and cyber culture continues to be both a benefit and a burden for public entities across the globe. It's no longer 1979 when the Buggles described how video transformed the music scene; it is 2014 and we face a new technology titan: cyber liability. Cyber liability risk is a complex and growing issue for entity leaders. Interest in this digital dilemma is especially high because, let's face it, cyber liability is way over our heads.

Read on for a sneak preview of top cyber liability risks, and hum the modern version of the Buggles' tune in your head: "I heard you on my smartphone back in 2012."

Cyber Liability Risks

1. **Forgotten Dark Data:** What happens to programs, documents, and other files that grow old on your obsolete CDs and perished computers? This decrepit stuff is known as 'dark data' because it hasn't seen the light of day in years. Unmanaged and forgotten, dark data poses a huge risk–it is usually inaccessible (aka not useful to you) and worse it is unprotected. Once you locate or identify your dark data, you'll be faced with a tough question: "What on earth should I do with it?" Your options may include destroying the data or storing and protect the data. Aim to establish clear policies that set data protection requirements as well as timelines for data storage.
2. **Poor BYOD Protocols:** Surely you know of BYOB, but what about Bring Your Own Device? Many employees use personal devices at work, or they access work materials on personal devices while at home. The innate risk of BYOD is that the organization must relinquish control of data management to its employees. That's a worrisome concept when, according to Info Tech Research Group, roughly 50% of data breaches are caused by user ignorance. An employee could fail to protect organizational data in any number of ways: losing a device that contains sensitive data; inadvertently exposing the entity's network to malware located on the employee's device; or, retaliating against the organization by deliberately destroying essential data.
   Your options are a bit tricky when it comes to protecting data on employee devices; in certain cases IT safeguards may be considered unlawful surveillance of employees. To balance employee privacy rights with data security needs, adopt a policy that specifies the information that employees may access from personal devices. Establish a simple system for employees to report lost or stolen devices, and consider maintaining access to devices so your IT team can wipe information immediately if a device is compromised.
3. **Useless or Harmful Tech Vendor Contracts**: Any contract is a danger if you don't fully understand it,

or if you agree to terms and conditions beyond your means. With tech contracts, be especially wary of impractical escape clauses and conditions requiring you to sacrifice rights to intellectual property. Another common concern is a tech vendor who assumes little liability or responsibility for client damages. Oftentimes, tech contracts provide a great protective limit for the vendor but not the client. Read every contract thoroughly and don't sign on any dotted lines until you're confident your organization is as protected as the vendor.

Erin Gloeckner is the former Director of Consulting Services at the Nonprofit Risk Management Center. NRMC welcomes your comments and inquires at info@nonprofitrisk.org or 703.777.3504.